

Stochastic motion planning for diffusions & fault detection and isolation for large scale nonlinear systems

Doctoral Thesis**Author(s):**

Mohajerin Esfahani, Peyman

Publication date:

2014-01

Permanent link:

<https://doi.org/10.3929/ethz-a-010163304>

Rights / license:

In Copyright - Non-Commercial Use Permitted

Dissertation ETH Zurich No. 21725

**Stochastic Motion Planning for Diffusions
&
Fault Detection and Isolation for Large Scale
Nonlinear Systems**

A dissertation submitted to
ETH Zurich

for the degree of
Doctor of Sciences

presented by

Peyman Mohajerin Esfahani

M.Sc., Sharif University of Technology, Tehran
born 21.03.1982 in Tehran
citizen of Iran

accepted on the recommendation of

Prof. Dr. John Lygeros, examiner
Prof. Dr. Halil Mete Soner, co-examiner
Prof. Dr. Karl Henrik Johansson, co-examiner

January, 2014

Abstract

The main theme of this thesis is twofold. First, we study a class of specifications, mainly the reachability type questions, in the context of controlled diffusion processes. The second part of the thesis is centered around the fault detection and isolation (FDI) problem for large scale nonlinear dynamical systems.

Reachability is a fundamental concept in the study of dynamical systems, and in view of applications of this concept ranging from engineering, manufacturing, biology, and economics, to name but a few, has been studied extensively in the control theory literature. One particular problem that has turned out to be of fundamental importance in engineering is the so-called “*reach-avoid*” problem. In the deterministic setting this problem consists of determining the set of initial conditions for which one can find at least one control strategy to steer the system to a target set while avoiding certain obstacles. The focus of the first part in this thesis is on the stochastic counterpart of this problem with an extension to more sophisticated maneuvers which we call the “*motion planning*” problem. From the technical standpoint, this part can be viewed as a theoretical bridge between the desired class of specifications and the existing numerical tools (e.g., partial differential equation (PDE) solvers) that can be used for verification and control synthesis purposes.

The second part of the thesis focuses on the FDI problem for large scale nonlinear systems. FDI comprises two stages: residual generation and decision making; the former is the subject addressed here. The thesis presents a novel perspective along with a scalable methodology to design an FDI filter for high dimensional nonlinear systems. Previous approaches on FDI problems are either confined to linear systems, or they are only applicable to low dimensional dynamics with specific structures. In contrast, we propose an optimization-based approach to robustify a linear residual generator given some statistical information about the disturbance signatures, shifting attention from the system dynamics to the disturbance inputs. The proposed scheme provides an alarm threshold whose performance is quantified in a probabilistic fashion.

From the technical standpoint, the proposed FDI methodology is effectively a relaxation from a robust formulation to probabilistic constraints. In this light, the alarm threshold obtained via the optimization program has a probabilistic performance index. Intuitively speaking, one would expect to improve the false alarm rate by increasing the filter threshold. The goal of the last part of the thesis is to quantify this connection rigorously. Namely, in a more general setting including a class of non-convex problems, we establish a theoretical bridge between the optimum values of a robust program and its randomized counterpart. The theoretical results of this part are finally deployed to diagnose and mitigate a cyber-physical attack introduced by the interaction between IT infrastructure and power system.

Zusammenfassung

Diese Dissertation besteht aus zwei Teilen. Zuerst wird eine Klasse von Spezifikationen für kontrollierte Diffusionsprozesse untersucht, vor allem mit Bezug auf Fragen der Erreichbarkeit. Der zweite Teil der Arbeit behandelt das Problem der Fehlererkennung und -isolierung (FDI) in grossen nichtlinearen dynamischen Systemen.

Erreichbarkeit ist ein fundamentales Konzept in der Untersuchung von dynamischen Systemen und wird als solches ausführlich in der Regelungstechnik behandelt. Anwendungen finden sich in verschiedensten Disziplinen wie den Ingenieurwissenschaften, der Systembiologie, der Produktionstechnik und der Ökonomie. Im Bereich der Ingenieurwissenschaften ist insbesondere das sogenannte “*Erreichbarkeit-Vermeidungsproblem*” von fundamentaler Wichtigkeit. Im deterministischen Fall besteht das Problem darin, die Menge der Anfangsbedingungen zu bestimmen, für welche mindestens eine Regelstrategie existiert, die das System in eine gegebene Zielmenge führt, wobei bestimmte Hindernisse zu vermeiden sind. Der Fokus des ersten Teils dieser Arbeit liegt auf dem stochastischen Pendant zu diesem Problem, ergänzt mit komplizierteren Zielvorgaben, das als “*Trajektorienplanungsproblem*” bezeichnet wird. Von einem regelungstechnischen Standpunkt her kann dieser erste Teil als theoretische Verbindung von der gewünschten Spezifikation des Reglers und der vorhandenen numerischen Software (z.B. Lösungsmethoden für partiellen Differentialgleichungen) betrachtet werden, die zur Synthese und Verifikation verwendet werden kann.

Der zweite Teil dieser Dissertation befasst sich mit dem FDI Problem für grosse nichtlineare dynamische Systeme. FDI besteht aus zwei Schritten: die Bestimmung der Regelabweichung sowie die Entscheidungsfindung, wobei der Fokus hier auf dem ersten Schritt liegt. Diese Arbeit präsentiert eine neue Sichtweise zusammen mit einer Methodik für den Entwurf eines FDI Filters für hochdimensionale nichtlineare Systeme. Bisherige Methoden für FDI Probleme beschränken sich entweder auf lineare Systeme oder sind nur für niedrigdimensionale Systeme mit spezifischer Struktur anwendbar. Im Gegensatz dazu wird ein optimierungsbasierter Ansatz für den Entwurf eines robusten Verfahrens zur Bestimmung der Regelabweichung vorgestellt, basierend auf statistischer Information über die Störsignale. Dieser Ansatz verschiebt die Sichtweise weg von der Systemdynamik und hin zu der Störgrösse. Er führt auf ein einfaches Schema, das einen Alarm liefert sobald ein bestimmter Schwellenwert überschritten wird, wobei die Güte dieses Schwellenwertes probabilistisch quantifiziert werden kann.

Von einem mathematischen Standpunkt aus gesehen stellt die vorgeschlagene FDI Methodik eine Relaxation von einer robusten zu einer probabilistischen Formulierung dar. Aus diesem Blickwinkel wird klar, weshalb der Schwellenwert, der durch die Lösung des Optimierungsproblems ermittelt wird, eine probabilistische Güte besitzt. Intuitiv betrachtet wird die Anzahl von Fehlalarmen bei einer Erhöhung dieses Schwellenwertes ansteigen. Das Ziel des letzten Teils

dieser Dissertation ist es, diesen Zusammenhang genauer zu untersuchen. Zu diesem Zweck wird gezeigt, wie in einem sehr allgemeinen Rahmen eine Schranke zwischen dem optimalen Zielfunktionswert eines robusten Optimierungsproblems und dem einer Näherungslösung mittels Stichproben hergeleitet werden kann. Schliesslich wird betrachtet, wie diese theoretischen Ergebnisse verwendet werden können, um cyberphysische Angriffe auf die Schnittstelle zwischen IT-Infrastruktur und Stromversorgungssystem zu erkennen und auszuschalten.